

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-290900

(43)Date of publication of application : 04.10.2002

(51)Int.Cl.

H04N 5/91
G06F 11/00
G06F 13/00
G06F 17/60

(21)Application number : 2001-085196

(71)Applicant : HITACHI LTD

(22)Date of filing : 23.03.2001

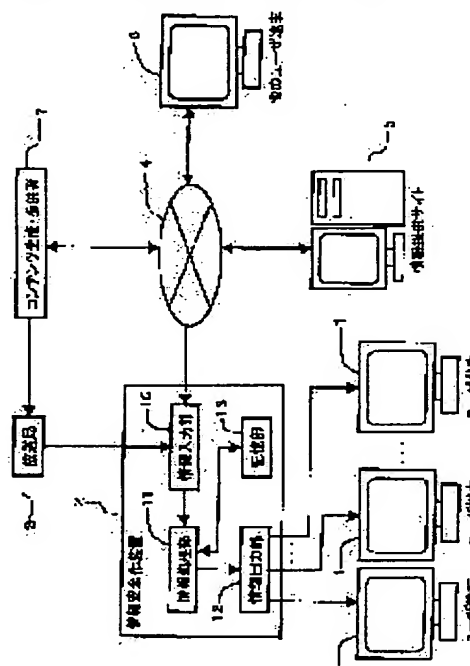
(72)Inventor : SANO KENJI

(54) INFORMATION SCREENING DEVICE AND INFORMATION GUARANTEE SYSTEM

(57)Abstract:

PROBLEM TO BE SOLVED: To prevent improper information from invading a user terminal which is arranged at home, etc.

SOLUTION: An information screening device 2 performs the unitary management of safety of information to be transmitted to a plurality of user terminals 1 and excludes improper information or adverse information, etc., at the border. Information transmitted from a broadcasting station 3 or an information providing site 5, etc., to the user terminals 1 is first received with the information input part 10 of the information screening device 2. Received information is checked with an information processing part 11 concerning a virus or contents. A screening processing such as the removal of virus data or the partial replacement of the contents is performed in improper information. The information processing part 11 gives a guarantee mark to information which is confirmed safe and an information output part 12 transmits the information to the user terminals 1.



LEGAL STATUS

[Date of request for examination]

27.12.2004

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's

BEST AVAILABLE COPY

decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号
特開2002-290900
(P2002-290900A)

(43) 公開日 平成14年10月4日 (2002. 10. 4)

(51) Int.Cl. ⁷	識別記号	F I	テ-マ-コ-ト (参考)
H 0 4 N 5/91		G 0 6 F 13/00	3 5 1 Z 5 B 0 7 6
G 0 6 F 11/00		17/60	3 0 2 E 5 B 0 8 9
13/00	3 5 1	H 0 4 N 5/91	P 5 C 0 5 3
17/60	3 0 2	G 0 6 F 9/06	6 6 0 N

審査請求 未請求 請求項の数17 O L (全 14 頁)

(21) 出願番号 特願2001-85196(P2001-85196)

(22) 出願日 平成13年3月23日 (2001. 3. 23)

(71) 出願人 000005108

株式会社日立製作所

東京都千代田区神田駿河台四丁目6番地

(72) 発明者 佐野 賢治

神奈川県横浜市戸塚区吉田町292番地 株式会社日立製作所デジタルメディア開発本部内

(74) 代理人 100095371

弁理士 上村 輝之 (外2名)

Fターム(参考) 5B076 FD08

5B089 GA11 GB02 KA17 KC47 KC51

KC52 KC53 KH28

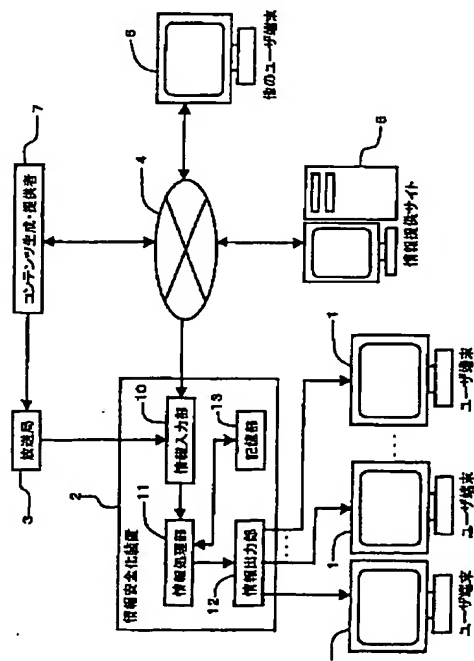
5C053 FA15 LA06 LA11 LA14

(54) 【発明の名称】 情報安全化装置及び情報保証システム

(57) 【要約】

【課題】 家庭内等に設置されたユーザー端末に不適切な情報が侵入するのを未然に防止すること。

【解決手段】 情報安全化装置2は、複数のユーザー端末1へ送信する情報の安全性を一元的に管理し、水際で不適切な情報や悪質な情報等を排除するものである。放送局3や情報提供サイト5等からユーザー端末1に向けて送信された情報は、まず情報安全化装置2の情報入力部10で受信される。受信された情報は、情報処理部11によってウイルスチェックやコンテンツの内容チェックが行われる。不適切な情報には、ウイルスデータの駆除やコンテンツの一部置換等の安全化処理が施される。情報処理部11は、安全が確認された情報に保証マークを与えて、情報出力部12からユーザー端末1に送信させる。



【特許請求の範囲】

【請求項1】 情報を供給する情報供給源と前記情報を利用する情報端末との間に設けられる情報安全化装置であって、
前記情報供給源から通信ネットワークを介して情報を受信する受信手段と、

前記受信した情報がユーザーの望まない情報（以下、不要情報）であるか否かを検査し、前記情報が不要情報であると判定した場合には、予め設定された所定の安全化処理を施す情報処理手段と、

前記不要情報以外の情報であると判定された情報及び前記安全化処理が施された情報を、予め設定された所定の情報端末に送信させる送信手段と、を備えたことを特徴とする情報安全化装置。

【請求項2】 前記検査された情報に、検査済みの情報であることを示す保証情報を付加する保証情報付加手段を更に備えた請求項1に記載の情報安全化装置。

【請求項3】 保証情報が対応付けられた情報が編集処理された場合には、前記保証情報を無効とする請求項2に記載の情報安全化装置。

【請求項4】 前記情報処理手段は、前記保証情報が付加された情報については、前記不要情報以外の情報であると判定する請求項3に記載の情報安全化装置。

【請求項5】 前記保証情報は、該保証情報が付加された情報を前記情報端末で利用する際に、ユーザーが認識可能に出力されるものである請求項2～請求項4のいずれかに記載の情報安全化装置。

【請求項6】 前記安全化処理が施された情報に、安全化処理済みであることを示す処理済み情報を付加する処理済み情報付加手段を更に備えた請求項1～請求項5のいずれかに記載の情報安全化装置。

【請求項7】 前記処理済み情報は、該処理済み情報が付加された情報を前記情報端末で利用する際に、ユーザーが認識可能に出力されるものである請求項6に記載の情報安全化装置。

【請求項8】 前記不要情報とは、前記情報端末に悪影響を及ぼす可能性のあるデータであり、前記安全化処理は、前記データを駆除するものである請求項1～請求項7のいずれかに記載の情報安全化装置。

【請求項9】 前記安全化処理は、前記情報端末に送信される情報の連続性が失われないように、前記不要情報を無力化するものである請求項1～請求項7のいずれかに記載の情報安全化装置。

【請求項10】 前記不要情報とは、閲覧が制限されている情報であり、前記安全化処理は、前記情報端末に送信される情報の連続性が失われないように、前記閲覧が制限されている情報を予め設定された置換用情報に置換するものである請求項9に記載の情報安全化装置。

【請求項11】 前記不要情報とは、前記情報端末に悪影響を及ぼす可能性のあるデータ及び閲覧が制限されて

いる情報であり、前記安全化処理は、前記情報端末に悪影響を及ぼす可能性のあるデータを駆除すると共に、前記情報端末に送信される情報の連続性が失われないように、前記閲覧が制限されている情報を予め設定された置換用情報に置換するものである請求項1～請求項7のいずれかに記載の情報安全化装置。

【請求項12】 前記情報処理手段は、前記不要情報以外の情報であると判定された情報及び前記安全化処理が施された情報を前記情報端末で選択して受信するためのメニュー情報を生成し、前記情報端末に提供する請求項1～請求項11のいずれかに記載の情報安全化装置。

【請求項13】 前記情報処理手段は、予め登録された各ユーザーの情報端末にそれぞれ送信する情報を該各ユーザーが予め指定した条件に応じてそれぞれ検査し、所定の安全化処理を施すものである請求項1～請求項12のいずれかに記載の情報安全化装置。

【請求項14】 ユーザーの望まない可能性のある情報（以下、不要情報）を含むコンテンツデータの生成方法であって、

20 時間圧縮された不要情報を生成するステップと、
前記不要情報を特定するための情報を該不要情報に対応付けるステップと、

前記不要情報に置換されるべき置換用情報を、前記不要情報の再生時間と同一時間となるように時間圧縮して生成するステップと、

前記不要情報と前記置換用情報とを対応付けるステップと、を含んでなるコンテンツデータの生成方法。

【請求項15】 ユーザーの望まない可能性のあるデータ（以下、不要データ）を時間圧縮して記録する第1の記録領域と、

30 前記第1の記録領域に対応付けて設けられ、前記不要データを特定するためのデータを記録する第2の記録領域と、

前記第1の記録領域に続けて設けられ、前記不要データに置換されるべき置換用データを、前記不要データの再生時間と同一時間となるように時間圧縮して記録する第3の記録領域と、を有するコンピュータ読取り可能な記録媒体。

【請求項16】 情報供給源から各情報端末に配信される情報の安全性を保証するための情報保証システムにおいて、

前記情報供給源と前記各情報端末との間には、該各情報端末へそれぞれ配信される情報の安全性を一元的に確認するための情報安全化装置を設け、

前記情報安全化装置は、

前記情報供給源から通信ネットワークを介して情報を受信する受信手段と、

予め各ユーザーがそれぞれ設定した検査条件に基づいて、前記受信した情報がユーザーの望まない情報（以下、不要情報）であるか否かを検査し、不要情報である

場合は予め設定された所定の安全化処理を施すと共に、前記検査又は安全化処理により安全であると判定した情報に保証情報を対応付けて出力する情報処理手段と、前記情報処理手段により安全であると判定された情報及び前記保証情報を、前記各情報端末に向けてそれぞれ送信される送信手段と、を備えて構成したことを特徴とする情報保証システム。

【請求項17】 情報供給源から情報端末へ配信される情報の安全性を、該情報端末が受信する前に検査するためのコンピュータプログラムにおいて、前記情報供給源から通信ネットワークを介して情報を受信させる機能と、前記受信された情報がユーザーの望まない情報（不要情報）であるか否かを検査する機能と、前記受信された情報が前記不要情報であると判定された場合には、予め設定された所定の安全化処理を施す機能と、前記受信した情報が前記不要情報以外の情報であると判定された場合には、該情報に保証情報を対応付ける機能と、前記保証情報が対応付けられた情報を前記情報端末に送信させる機能と、をコンピュータ上に実現させるためのコンピュータプログラム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、ユーザーが利用する各種の情報端末に供給される情報の安全性を事前に検査し、必要な安全化処置を施してから前記情報端末に送信させる情報安全化装置及び情報保証システムに関する。

【0002】

【従来の技術】ユーザーは、例えば、テレビジョン受像機、パーソナルコンピュータ、携帯情報端末（携帯電話を含む）等のような各種の情報端末を用いることにより、ネットワークを介して供給される各種のコンテンツを閲覧し、利用等することができる。しかし、各種のコンテンツの中には、ユーザーにとって好ましくないものも存在する。

【0003】例えば、インターネット等の広域大規模通信ネットワークを介して、電子メールをやり取りしたり、無償又は有償で配布されているプログラムやコンテンツ（映像等）をダウンロードしたりする場合を例に挙げると、受信したデータ（プログラムを含む）中に、いわゆるコンピュータウイルスが含まれていることもある。

【0004】また、例えば、テレビ放送を例に挙げると、受信した映像の一部又は全部に、過激な暴力場面や性的描写場面が含まれていることがあるが、このような刺激の強い場面の映像は、全てのユーザーに受け入れられるわけではない。例えば、青少年のいる家庭では、こ

のような映像の視聴を望まない。

【0005】そこで、従来は、例えば、情報端末にインストールされたいわゆるワクチンソフトによって、情報端末が受信した情報ファイルのウイルス感染を検査している。また、放映される場面がユーザーにとって適正なものであるか否かについては、保護者等が予め放送内容を視聴して判断し、不適切と判断した場合について外部操作により視聴を規制する技術も知られている。

【0006】

10 【発明が解決しようとする課題】ユーザーは、受信した情報がコンピュータウイルスに感染しているか否か予め知ることができないので、全ての受信情報について検査する必要がある。即ち、たとえ情報供給元の信頼性が高い場合であっても、受信情報の安全性についてユーザー側では確認できないため、全ての受信情報を検査しなければならない。また、ウイルスパターンは、日々変化するため、ユーザーは、常に最新のウイルス情報を入手してワクチンソフトを更新しなければならない。このため、ユーザー側の作業が煩雑化し、使い勝手が悪い。

20 【0007】一方、予め放送内容を視聴し、不適切と判断した場合について外部操作により視聴を規制する方法では、ユーザーの作業が煩雑であり、やはり使い勝手が低い。また、過激な場面の終了を予測するのが難しく、視聴可能な場面まで規制される可能性もある。

【0008】さらに、近年では、テレビジョン放送とデータ通信とが融合したり、インターネット接続の可能なテレビジョン受像機やテレビ放送が視聴可能なパーソナルコンピュータ等が普及している。また、一家に一台の情報端末を所有する時代から一人一台の時代を経て、一人が複数種類の情報端末を所有する時代を迎えている。従って、ユーザー、特に、未成年の家族と同居する親や教育者あるいは監督者等は、多種類の情報端末を介して配信される多くの受信情報の全てについて、その安全性を事前に確認する必要がある、大変煩雑な作業を強いられる。

30 【0009】本発明は、上述した種々の問題に鑑みてなされたもので、その目的は、情報端末に受信される前に、該情報端末に配信された情報の安全性を確認するための情報安全化装置及び情報保証システムを提供することにある。本発明の他の目的は、安全性が確認された情報に保証を与え、安全な情報の流通を円滑化できるようにした情報安全化装置及び情報保証システムの提供にある。本発明の更なる目的は、後述する実施の形態の記載から明らかになるであろう。

【0010】

40 【課題を解決するための手段】上記課題を解決するために、本発明に係る情報安全化装置は、情報を供給する情報供給源と情報を利用する情報端末との間に設けられる。この情報安全化装置は、情報供給源から通信ネットワークを介して情報を受信する受信手段と、受信した情

報がユーザーの望まない情報（以下、不要情報）であるかを検査し、不要情報であると判定した場合には、予め設定された所定の安全化処理を施す情報処理手段と、不要情報以外の情報であると判定された情報及び安全化処理が施された情報を、予め設定された所定の情報端末に送信させる送信手段とを備える。

【0011】ここで、「情報」としては、例えば、地上波や衛星又はケーブル等を介したテレビジョン放送の放映内容、インターネット等を利用する電子メール、ウェブページ、プログラム、映像データ、音楽データ等の種々のものを挙げることができる。従って、「情報供給源」としては、例えば、テレビ局、ウェブサイト、ネットワークに接続された他の情報端末等を挙げることができる。「ユーザーの望まない情報」とは、積極的又は消極的にユーザーが受信を希望しない情報の意味であり、具体的には、例えば、情報端末に悪影響を及ぼすおそれのあるプログラムやデータ（いわゆるコンピュータウイルス）や、未成年者等に視聴が規制されている過激な場面の映像や音声等のような不適切な情報、不適正な情報、悪質な情報を挙げることができる。

【0012】情報安全化装置は、情報端末と情報供給源との間に位置して、情報端末が情報を受信する前に、全ての情報の安全性を検査する。不要情報の場合は、所定の安全化処理を施してから情報端末に送信する。これにより、情報端末を利用するユーザー自身は、ウイルス情報の更新や、好ましくない場面の事前検閲等を行う必要がない。

【0013】好適な実施形態によれば、保証情報付加手段は、検査された情報に検査済みの情報であることを示す保証情報を付加する。

【0014】そして、保証情報が付された検査済みの情報がユーザーの情報端末で編集処理された場合には、保証情報は無効とされる。検査済みの情報に操作が加えられることにより、安全性を保証し得なくなるためである。ここで、保証情報を無効にするとは、例えば、保証情報を削除する場合のほか、保証情報自体は存続させて有効性を示す値を0に設定する場合も含む。

【0015】検査後に操作が加えられた場合に保証情報を無効とすることにより、保証情報に対する信頼性がより高まる。そこで、情報処理手段は、保証情報が付加された情報については、不要情報以外の情報であると直ちに判定することができる。例えば、ある一群の情報端末の安全性を一元的に管理する情報安全化装置によって検査され保証情報が付加された情報が、他の一群を構成する情報端末に転送された場合、該他の一群の情報端末の安全性を統括する情報安全化装置では、何ら検査することなく、この保証情報付きの情報を安全なものとして受け入れることが可能である。

【0016】好適な実施形態では、保証情報は、該保証情報が付加された情報を情報端末で利用する際に、ユー

ザーが認識可能に出力される。「ユーザーが認識可能に出力」とは、ユーザーが五官で保証情報の存在を感知できるように出力することを意味し、具体的には、例えば、ディスプレイ装置に表示出力されるマークやコメント、スピーカーに音声出力される鳴動音やメッセージ等を挙げることができる。

【0017】また、不要情報を無力化する安全化処理が施された情報についても、安全化処理済みであることを示す処理済み情報を付加することができる。そして、この処理済み情報もユーザーが認識可能に出力するのが好ましい。

【0018】好適な実施形態では、安全化処理は、情報端末に送信される情報の連続性が失われないように、不要情報を無力化するようにになっている。「情報の連続性が失われないように」とは、情報端末が既に受信した部分とこれから受信する部分との時間経過上の連続性、一体性が損なわれないようにすることを意味する。

【0019】例えば、不要情報として、閲覧が制限されている情報を挙げると、安全化処理は、情報端末に送信される情報の連続性が失われないように、閲覧が制限されている情報を予め設定された置換用情報に置換する。なお、置換用情報は、閲覧が制限されている情報と同一の再生時間となるように圧縮されているのが好ましい。さらに、置換用情報は、例えば、過激な情景描写を廃し、ストーリーの把握に支障を与えないような情報として加工されているのがより望ましい。

【0020】好適な実施形態では、検査済み又は安全化処理済みの情報は、無条件で直ちに情報端末に送信されるのではなく、受信情報を選択するためのメニュー情報に基づいて、ユーザーは、受信を希望する情報を選択するようになっている。

【0021】好適な実施形態によれば、情報処理手段は、予め登録された各ユーザーの情報端末にそれぞれ送信する情報を該各ユーザーが予め指定した条件に応じてそれぞれ検査し、所定の安全化処理を施すようになっている。

【0022】本装置によるサービスを希望する各ユーザーは予め登録する必要がある。各ユーザーは、情報の安全性に関する条件をそれぞれ指定できる。具体的には、例えば、「成人指定」等のような視聴規制のある放送内容の場合、各情報端末を利用する視聴者の年齢層によって、安全性の判断は異なる。そこで、情報処理手段は、各ユーザーが予め登録した条件に基づいて、安全性をそれぞれ判断する。本装置によるサービスの開始及び停止は、各ユーザーがそれぞれ自由に設定することが可能である。

【0023】時間圧縮された不要情報を生成するステップと、不要情報を特定するための情報を該不要情報に対応付けるステップと、不要情報に置換されるべき置換用情報を、不要情報の再生時間と同一時間となるように時

間圧縮して生成するステップと、不要情報と置換用情報とを対応付けるステップとによって、不要情報を含んだコンテンツデータを生成することができる。

【0024】不要情報と置換用情報とを時間圧縮することにより、圧縮情報を伸長して再生する時に生じる時間差分を利用して、時間の連続性を損なわずに不要情報を置換用情報に置き換えることができる。どの部分が不要情報であるかを特定するための情報は、コンテンツデータの先頭に設けてもよいし、不要情報の先頭に設けてもよい。不要情報を特定するための情報を検出することにより、不要情報を置換用情報に置き換えることができる。

【0025】

【発明の実施の形態】以下、図1～図11に基づき、本発明の実施の形態を説明する。図1は、情報安全化装置を備えた情報保証システムの全体を概略的に示す構成説明図である。

【0026】各ユーザーの使用する「情報端末」としてのユーザー端末1は、情報安全化装置2にそれぞれ接続されている。ユーザー端末1としては、例えば、テレビジョン受像機、パーソナルコンピュータ、携帯情報端末（携帯電話を含む）等を挙げることができる。各ユーザー端末1は、少なくとも出力手段及び操作手段をそれぞれ備えている。出力手段としては、例えば、モニタディスプレイ装置やスピーカ等を挙げることができる。操作手段としては、例えば、キーボードスイッチ、ポインティングデバイス、マイクロフォン等を挙げることができる。ユーザー端末1がパーソナルコンピュータやワークステーション又は携帯情報端末のようなマイクロコンピュータシステム製品として構成される場合、該ユーザー端末1は、情報安全化装置2を経由して受信した情報を編集したり、新たな情報を生成して発信することもできる。

【0027】各ユーザー端末1は、情報安全化装置2を介してテレビ放送やインターネットからのデータ等を受信する。情報安全化装置2は、予め登録された複数のユーザー端末1へ送信する情報の安全性をそれぞれ個別に管理することができる。例えば、集合住宅の各家庭にそれぞれ設置されたユーザー端末1を一台の情報安全化装置2によって管理できるし、または、一家庭内に設置された複数のユーザー端末1を家庭内に設置した情報安全化装置2によって管理することもできる。これに限らず、各ユーザー端末1毎に情報安全化装置2を設ける構成としてもよい。

【0028】情報安全化装置2は、各ユーザー端末1へ不適切、不適正な情報が配信されるのを水際で防止すべく、各ユーザー端末1と通信ネットワーク4との間に設けられる。通信ネットワーク4としては、例えば、公衆電話回線等を使用したインターネット網を挙げることができる。また、情報安全化装置2は、衛星通信や地上波

又はケーブル伝送等を介して、「情報供給源」の一つである放送局3が放映する番組を受信することができる。

【0029】通信ネットワーク4には、「情報供給源」としての情報提供サイト5、他のユーザー端末6及びコンテンツ生成・提供者の装置（以下「コンテンツ提供装置」）7が接続されている。情報提供サイト5は、例えば、HTMLやXML等で記述されたウェブページやプログラム等の各種情報をHTTPやFTP等の所定のプロトコルにより提供する。他のユーザー端末6としては、例えば、パーソナルコンピュータやワークステーションあるいは携帯情報端末等を挙げることができる。他のユーザー端末6から情報安全化装置2の管理下にある各ユーザー端末1に向けて電子メール等の情報を送信することができる。コンテンツ提供装置7は、例えば、映画やドラマ又はニュース等の各種映像番組、音楽番組、ラジオ番組を生成して配信するものである。コンテンツ提供装置7が提供する各種のコンテンツは、通信ネットワーク4を介して、又は放送局3から情報安全化装置2に送信される。

【0030】次に、情報安全化装置2の構成について、図1及び図2を参照しつつ説明する。情報安全化装置2は、「受信手段」としての情報入力部10と、「情報処理手段」としての情報処理部11と、「送信手段」としての情報出力部12と、「記憶手段」として表現可能な記憶部13とから大略構成されている。

【0031】情報入力部10は、例えば、テレビ放送やデータ通信等の各種情報を受信可能に構成されており、各ユーザー端末1宛の情報をそれぞれ並列に受信処理可能である。情報処理部11は、コンピュータ資源を利用して、受信した情報の安全性を検査し、ユーザーの望まない不適切又は不適正な情報（不要情報）を安全化する場合がある。

【0032】図2に示すように、情報処理部11は、「検査手段」として表現可能な検査部21と、「安全化処理手段」として表現可能な安全化処理部22と、「保証情報付加手段」及び「処理済み情報付加手段」としての保証マーク付与部23とを備えている。

【0033】検査部21は、受信した情報の安全性を検査するものである。検査部21は、各ユーザーが予め設定した検査条件に基づいて、各受信情報の安全性をそれぞれ判断する。ユーザー毎の検査条件は、記憶部13内に形成されるユーザー管理データベースで管理することができる。ここで、検査部21は、各ユーザーの指定した検査条件に無条件で従う必要はない。例えば、受診情報がコンピュータウイルス等のようにコンピュータ資源に致命的な悪影響を与える可能性を有する場合は、ユーザー指定条件にかかわらず、不要情報であると判定することができる。

【0034】検査部21は、各受信情報の特性（性質、種類）に応じて安全性をそれぞれ判断するものである。

例えば、データ（プログラムを含む）を受信した場合、検査部21は、この受信データ中に予め登録されたウイルスパターンが存在するかどうかをパターンマッチング法等によって検査する。ウイルスチェックに用いるウイルスパターンデータは、記憶部13内に形成されるウイルス管理データベースで管理することができる。なお、このウイルス管理データベースは、定期的に又は不定期に最新の情報に自動更新される。ウイルスパターンの更新は、ウイルスパターンを提供する情報提供サイト5からの通知（プッシュ型更新）、又はウイルス管理データベースから情報提供サイト5への最新ウイルスパターンの問合せ（プル型更新）等により行うことができる。また、ウイルスを含むデータを通信ネットワーク4から受信した場合、検査部21は、ウイルスを含有するデータの送信元やウイルス情報を管理するサイト等に対して警告メッセージを送信する機能を有する。

【0035】テレビ放送や通信ネットワーク4から映像情報を受信した場合、検査部21は、後述するように、不要情報の存在を示すランク情報の有無を検出し、ランク情報を検出した場合は、不要情報であると判定する。また、検査部21は、検査済み又は安全化処理済みであることを示す保証マークが付加された情報については、不要情報以外の情報として、即ち安全な情報であると判断する。

【0036】安全化処理部22は、各受信情報の特性に応じた安全化処理を行うものである。例えば、不要情報がコンピュータウイルス等のように、本来の情報に付加された冗長な情報である場合、安全化処理部22は、冗長な情報を削除することにより安全化処理を施す。例えば、映像の一部に過激な場面等の不要情報が存在する場合、安全化処理部22は、後述のように、不要情報に対応付けられている置換用情報で不要情報を置き換えることにより安全化処理を施す。安全化処理部22は、圧縮された情報をソフトウェア又はハードウェアによって伸長させる伸長手段を備えている。なお、映像等の圧縮情報は、いったん記憶部13内のコンテンツ格納部に蓄積させてから伸長することができる。

【0037】保証マーク付与部23は、検査部21によって安全であると判定された情報及び安全化処理部22によって安全化処理された情報について、情報の安全性を示す保証マークを付加するものである。図3と共に後述するように、保証マークのデータには、コピー管理データが付随する。保証マークが対応付けられた情報がユーザー端末1上で編集処理された場合は、保証マークは無効となる。ここで、留意すべき点は、保証マーク付与部23は、予め用意された複数種類の保証マークデータのうち、受信情報の特性に応じて又は複数の保証マークを付加させる点である。例えば、コンピュータウイルスが含まれていない情報に対しては「ウイルス検査済みマーク」を、ウイルスが除去された情報については「ウ

イルス除去済みマーク」を、過激な場面を穏当な置換用情報に置き換えた場合は「置換済みマーク」を、それぞれ付加することができる。映像が通信ネットワーク4を介してデータ通信で配信された場合には、例えば「ウイルス検査済みマーク」と「置換済みマーク」のように、一つの情報に複数種類のマークが付加される場合もある。

【0038】情報出力部12は、安全であると判定された情報及び安全化処理された情報を、予め登録された所定のユーザー端末1に向けて送信する。即ち、情報出力部12は、安全な情報のみを各ユーザー端末1に送信する。また、情報出力部12は、予め情報保証サービスを申し込んでいるユーザーの端末1に対してのみ情報を送信する。情報出力部12と各ユーザー端末1とは、例えば、有線又は無線式のLAN（Local Area Network）、公衆電話回線網等の種々の通信媒体を介して接続可能である。

【0039】情報安全化装置2は、上述の構成に加えて、各ユーザー端末1からの情報転送要求を処理するための手段も備えている。情報要求受付部31は、例えば、テレビチャンネルの番号、URL（Uniform Resource Locator）、電子メールアドレス、電話番号等の各種情報取得に必要な要求を各ユーザー端末1からそれぞれ受け付けるものである。受け付けられた情報転送要求は、情報要求発行部32により所定の情報供給源に送られる。

【0040】次に、図3及び図4を参照して、データ構造等につき説明する。まず、図3は、検査済み又は安全化処理済みの情報（コンテンツ）に保証マークを対応付けて送信する場合のデータ構造を概略的に示す模式図である。

【0041】情報処理部11が出力するデータは、図3（a）に示すように、4種類のデータ記憶領域D1～D4を有する。先頭に位置する識別データ領域D1には、検査等された情報の供給元を特定する情報と、宛先のユーザー端末1を特定する情報と、データ種別を示す情報と、データ長を示す情報等の識別データが格納されている。マークデータ領域D2には、保証マーク付与部23により付加された一つ又は複数の保証マークのデータが格納されている。なお、保証マークのデータ自体を直接格納するのではなく、ユーザー端末1側に予めインストールされた保証マークのデータを特定するための情報でもよい。コピー管理領域D3には、保証マークのコピー制限を行うためのデータが格納されている。検査済み又は安全化処理済みのコンテンツが編集処理され改変された可能性がある場合、コピー管理データは「コピー不可」にセットされる。これにより、編集処理されたコンテンツに保証マークデータは付加されない。コンテンツの編集処理を行わず、ユーザー端末1側のローカルディスクに単純に記憶させたような場合は、コンテンツ再生

時に保証マークのデータも再現される。なお、コピー管理データによって、コンテンツの著作権管理を併せて行うようにしてもよい。

【0042】図3(b)には、ユーザー端末1側での表示状態の一例が示されている。ユーザー端末1のディスプレイ装置には、検査済み又は安全化処理済みのコンテンツが保証マークと対応付けられて一覧形式で表示される。即ち、図3(b)は、受信を希望するコンテンツを選択する選択メニュー画面であって、保証マークとコンテンツ名とを対応付けて一覧表示させることにより、ユーザーは、情報受信前に、コンテンツの内容や安全性等を予め確認することができるようになっている。ユーザーは、一覧表示された各コンテンツの中から、受信を希望するコンテンツを選択することができる。例えば、ダイレクトメールと思われる場合、ユーザーは、このコンテンツの受信を拒否することができる。ユーザーがコンテンツを選択すると、保証マークと共に、コンテンツの内容がディスプレイ装置に表示される。保証マークは、コンテンツの視聴を妨げないように、目立たない位置に表示させることができる。また、保証マークは、コンテンツの視聴中に常時表示させても良いし、最初の所定時間だけ表示させてもよい。

【0043】次に、図4は、閲覧が規制されている情報を含むコンテンツのデータ構造及び再生方法を概略的に示す説明図である。

【0044】ここで、図中に示すオリジナルデータDA～DCとは、映像等のオリジナル場面のデータであり、それぞれデジタル化されて時間圧縮されている。ランク情報とは、過激な場面等の視聴に不適切な部分を特定するための情報であり、ランク付けの情報(例えば、13歳未満視聴不可、18歳未満視聴不可、20歳以上視聴可等)と、不適切なデータの範囲を特定するための情報(例えば、バケット番号やデータ長等)と、ランク情報に対応するランク対応情報(D14)を特定するための情報とを備えている。図4の例では、オリジナルデータDBを規制されるべき場面のデータとして示している。ランク対応情報は、規制されるべきデータに置換するための置換用データDBXを識別するものである。

【0045】図4(a)に示すように、ユーザーが予め設定した条件、即ち視聴ランクがランク情報中のランクよりも高い場合は、オリジナルデータDAに続いて、オリジナルデータDBが伸長され、ユーザー端末1に配信される。逆に、ユーザーの設定した視聴ランクがランク情報中のランクよりも低い場合は、オリジナルデータDBに代えて、置換用データDBXが伸長されてユーザー端末1に配信される。

【0046】ここで、注意すべき点は、オリジナルデータDBと置換用データDBXとは、伸長して再生される開始時刻(T0)、終了時刻(T1)、再生時間(T0-T1)が同一となるように設定されている点である。

各データDA～DC及びDBXは、それぞれ圧縮された状態で情報供給源から受信されるため、非圧縮状態のデータを再生する時間と圧縮データを伸長して再生する時間との差分を利用して、置換データDBXの開始時刻及び終了時刻をオリジナルデータDBのそれと一致させることができる。これにより、コンテンツの再生時間経過上の連続性は保持される。

【0047】なお、これに限らず、置換データDBXは、オリジナルデータDBとは別にして受信しておき、置換時に入れ替えるようにしてもよい。この場合は、各データを圧縮する必要はない。また、各データがバケット化されている場合は、各バケットにバケットデータの属性を示す情報(オリジナルデータか置換用データか)と、ランク情報(オリジナルデータのバケットのみ)と、オリジナルデータのどのバケットに対応するのかを示す情報(置換用データのバケットのみ)等の識別データをそれぞれ付加しておけばよい。この識別データによってバケットを分別し、ユーザーの設定したランクに応じてデータの入れ替え処理を行うことができる。ユーザーの設定したランクが低い場合、識別データ中にランク情報の設定されていないバケットはそのまま伸長して再生し、ランク情報の設定されたバケットは破棄し、置換用データのバケットのみを選択して伸長再生すればよい。

【0048】置換用データの内容としては、種々のものを採用することができる。「13未満の視聴が規制されています」等のメッセージを表示させるだけでも良いが、視聴規制に触れない範囲内で、ストーリー等の流れが把握できるような穏当な内容として置換用データを構成するのが好ましい。具体的には、視覚的に刺激的な場合は、アニメーション化したり、ワイヤーフレームモデルで表現することにより、ストーリーの連続性を保持したまま穏当な内容に変更することが可能である。聴覚的に刺激的な場合は、音声の一部消去や吹き替え、字幕等で対応可能である。

【0049】次に、図5～図9に基づいて、本実施の形態の処理の流れを説明する。まず、図5は、受信情報中にコンピュータウイルスが含まれていた場合の説明図である。

【0050】ユーザーが、端末1を介して電子メールやプログラム等の情報取得を情報安全化装置2に要求すると(P1)、この情報転送要求は情報安全化装置2を介して所定の情報供給源に送信される(P2)。情報供給源から送信された情報を情報安全化装置2が受信すると(P3)、情報安全化装置2は、受信情報を検査する(P4)。検査の結果、コンピュータウイルスが検出された場合は、情報安全化装置2によってウイルスが駆除されると共に(P5)、情報安全化装置2から情報供給源や関係機関に対してウイルス発見の警告メールが送信される(P6)。

【0051】情報安全化装置2は、ウイルスを駆除した情報に保証マークを付加して(P7)、ユーザー端末1に送信する(P8)。次に、ユーザー端末1により発行された新たな情報転送要求に応じて(P9、P10)、情報供給源から情報安全化装置2に送信された情報に保証マークが付加されている場合(P11)、情報安全化装置2は、保証マークの有無だけを検査し(P12)、この受信情報をユーザー端末1に送信する(P13)。

【0052】図6は、過激な場面等を含んだ映像等の情報を処理する場合の説明図である。ユーザーからの情報転送要求に応じて(P21、P22)、情報供給源から情報安全化装置2に圧縮された映像情報が送信される

(P23)。情報安全化装置2は、ユーザーが予め設定したランクに基づいて、受信した映像情報をそのまま配信するか否かを判定する(P24)。ランク情報が設定されていない映像情報については、安全化処理部22により圧縮映像情報を伸長してユーザー端末1に送信する(P25、P26)。一方、ランク情報の設定された映像情報及び該映像情報に置換される置換用情報が、情報供給源から情報安全化装置2に送信されて場合は(P27、P28)、映像情報中のランク情報を検査し(P29)、ユーザー設定ランクよりも映像情報の設定ランクの方が高い場合は、置換用情報に入れ替る(P30)。そして、置換用情報に保証マークを付加して(P31)、ユーザー端末1に送信する(P32)。

【0053】次に、図7～図9は、処理の流れを示すフローチャートである。なお、これらの各フローチャートは、処理の概要を示すもので、実際のプログラム構造とは相違する。

【0054】図7は、コンピュータウイルスをチェックするための処理を示す。まず、通信ネットワーク4を介して電子メールやウェブページ又はプログラム等のコンテンツを受信すると(S1)、この受信したコンテンツに保証マークの一種である検査済みマークが付加されているか否かを検査する(S2)。検査済みマークが付加されている場合(S2:YES)は、後述のS3～S8の各ステップを省略してS10に移行する。一方、受信したコンテンツに検査済みマークが付加されていない場合は、既知のウイルスパターンとのパターンマッチングが行われる(S3)。

【0055】パターン照合によりコンピュータウイルスが検出されなかった場合(S4:NO)は、検査済みマークを付加する(S5)。コンピュータウイルスが検出された場合は(S4:YES)、このウイルスを除去し(S6)、保証マークの一種である処理済みマークをコンテンツに付加する(S7)。そして、付加されたマークにコピー制限の情報を更に設定し(S8)、保証マークとコンテンツを対応付けて(S9)、受信選択用のメニューを生成し(S10)、この受信選択用メニューをユーザー端末1に送信する(S11)。ユーザーがメニューに基づ

いて受信を希望する情報を選択すると(S12:YES)、ユーザーにより選択された情報のみがユーザー端末1に送信される(S13)。なお、ユーザーにより選択されなかった情報は、ユーザーからの指示に基づいて破棄することもできるし、所定期間だけ記憶部13に保存した後、自動的に破棄することもできる。

【0056】次に、図8は、視聴が規制されている場面を含んだ映像等のコンテンツを配信する場合の処理を示す。

【0057】まず、通信ネットワーク4を介して映像データを受信すると(S21)、受信データ中にランク情報が設定されているか否かを検査する(S22)。ランク情報が設定されていない場合(S22:NO)は、穏当な内容のデータであるから、S25に移行して受信データを伸長させる。ランク情報が付加されている場合は、ランク情報中の規制ランクとユーザーが設定したランクとを比較し、規制ランクがユーザー設定ランクを上回っているか否かを判定する(S23)。規制ランクの方が高く設定されている場合は、置換用データに入れ替えて(S24)、伸長処理を行う(S25)。伸長されたデータは、送信タイミングが到来したときにユーザー端末1に送信される(S26、S27)。

【0058】次に、図9は、ユーザー端末1側の受信処理を示す。まず、ユーザー端末1は、情報安全化装置2が提供する受信選択用のメニュー情報を受信する(S31)。

【0059】ユーザーは、表示されたメニューに基づいて(S32)、受信を希望するコンテンツを選択する(S33)。ユーザーがコンテンツを選択すると、この選択されたコンテンツの転送が情報安全化装置2に要求される(S34)。情報安全化装置2からコンテンツを受信すると(S35:YES)、受信されたコンテンツがユーザー端末1のディスプレイ装置に表示される(S36)。コンテンツの閲覧を終えたユーザーは、閲覧終了に際して、コンテンツデータをユーザー端末1のローカルディスクに保存するか否かを選択することができる(S37)。コンテンツを保存する場合、コンテンツが編集されたか否かを判定し(S38)、編集されていた場合(S38:YES)、保証マークを無効にすべくコピー管理情報を「コピー不可(禁止)」に設定させる(S39)。

【0060】このように構成される本実施の形態によれば、以下の効果を奏する。

【0061】ユーザー端末1が情報を受信する前に、情報安全化装置2によって情報の安全性を検査し、必要な安全化処理を行うため、ユーザー端末1側でウイルスチェックやウイルスパターンデータの更新作業等を行う必要がない。これにより、ユーザー側での煩雑な作業を廃して、安全な情報のみを受信することができ、使い勝手

【0062】検査済みマーク、安全化処理済みマーク等の保証マークが付加された情報を情報安全化装置2からユーザー端末1に送信するため、保証マークによってユーザーに安心感や信頼感を与えることができる。

【0063】検査等された情報が編集処理された場合は、保証マークを無効とするため、保証マークの信頼性を高めることができ、ひいては、保証マークの付加された情報についての実質的な検査を省略して速やかに情報をユーザー端末1に送信することができる。

【0064】コンピュータウイルス及びテレビ放送という異なる種類の情報を情報安全化装置2で処理できるため、システムをコンパクトに構成することができ、使い勝手も高まる。

【0065】安全性が確認された情報を直ちにユーザー端末1に送信するのではなく、受信選択用メニューを介してユーザーが選択した情報を情報安全化装置2からユーザー端末1に送信するため、ウイルスチェック等では排除しきれない不要な情報をユーザーの判断によって排除することができ、使い勝手が向上する。

【0066】予め情報保証サービスを希望している複数のユーザー端末1への情報配信を一台の情報安全化装置2によって一元的に管理できるため、図10に示すように、情報保証サービス停止中のユーザー端末1については、情報安全化装置2による保証は行われない。換言すれば、各ユーザー端末1は、情報安全化装置2をいわゆるレンタルファイアウォールのように利用することができる。即ち、各ユーザーは、必要と判断するときだけ、情報保証サービスを利用することが可能である。但し、実施の形態の記載から明かなように、本発明の情報安全化装置2は、単なるファイアウォールとは異なり、種々の利点を備えている点に注意すべきである。

【0067】図11に示すように、例えば、情報安全化装置2をISP (Internet Service Provider) の装置41に設置し、インターネット接続契約を結んだユーザーを管理する顧客データベース42と連動させることにより、ユーザー端末1は、公衆電話回線網 (PSTN) 43等を介して安全な情報のみを受信することができる。

【0068】次に、図12に基づいて本発明の第2の実施の形態を説明する。図12は、ユーザーによっては規制されるべき不適切な場面を含んだコンテンツを、本情報保証サービスで利用可能な形態で生成する場合の処理の流れを概略的に示すものである。

【0069】まず、映画やドラマ等のコンテンツを生成した後 (S41)、このコンテンツの内容をチェックして規制すべき場面にランク情報を対応付ける (S42)。次に、ランク情報が対応付けられた場面のデータに入れ替えるべき置換用データを生成する (S43)。そして、オリジナルのデータと置換用データとを対応付けた後 (S44)、コンテンツを保存し、通信媒体や記録媒体を介して供給する (S45)。

【0070】なお、本発明は、上述した実施の形態に限定されない。当業者であれば、実施の形態で述べた構成に新たな構成要素を追加したり、削除したり、変更等したりして種々の変形を行うことができる。

【0071】例えば、情報安全化装置2の提供する情報保証サービスが有料である場合等には、情報出力部12から送信する情報を暗号化し、ユーザー端末1側でそれぞれ復号化するように構成することもできる。これにより、情報安全化装置2から複数のユーザー端末1に同一の情報を一斉に送信した場合でも、所定の暗号鍵を保有するユーザー端末1だけが情報を利用することができる。

【0072】また、ユーザーは、複数の検査条件 (規制ランク等) を予め設定することができ、時間帯や曜日等のパラメータに応じて検査条件を切り替えることも可能である。例えば、指定された曜日の指定されて時間帯については視聴規制を緩めたり、厳しくしたりすることができる。

【0073】また、複数の置換用情報を用意しておき、ユーザーの希望に応じて情報の入れ替えを行うように構成することもできる。

【0074】さらに、置換情報が用意されていない場合は、ソフトウェア又はハードウェアにより構成されたローパスフィルタを用いてオリジナル情報の低周波成分のみを抽出し、ユーザー端末1に送信するように構成することも可能である。あるいは、オリジナル情報の各フレームから動きのベクトルを抽出し、予め用意された代替オブジェクトを検出されたベクトルに基づいて動作させることにより置換情報を自動的に生成することもできる。

【0075】さらに、前記実施の形態では、放送で送られてくる以外の情報と、放送で送られてくる情報とに分けて述べたが、それぞれで説明した情報の処理や情報の扱いは、送られてくる方式で区別する必要はない。

【0076】また、情報安全化装置2とユーザー端末1とは、それぞれ別体に形成し分離配置する場合を例示したが、両者を一体化してもよい。

【0077】

【発明の効果】以上詳述した通り、本発明によれば、情報端末は、事前に安全性が確認され、必要な処理が施された情報のみを受信することができ、使い勝手等が向上する。

【図面の簡単な説明】

【図1】本発明の実施の形態に係る情報安全化装置を用いた情報保証システムの全体構成を概略的に示す構成説明図である。

【図2】情報安全化装置の機能構成を示すブロック図である。

【図3】保証マークとコンテンツデータとの関係を示す説明図であって、図3 (a) はデータ構造を示し、図3

(b) はユーザー端末側での表示例を示す。

【図4】視聴が規制されるべき場面を含んだコンテンツを再生する場合の説明図であって、図4(a)は置換用データに入れ替えずに再生する場合を、図4(b)は置換用データに再生する場合をそれぞれ示す。

【図5】放送以外のデータとしてコンピュータウイルスを処理する場合の全体の流れを示す説明図である。

【図6】映画等の放送データを処理する場合の全体の流れを示す説明図である。

【図7】コンピュータウイルスを検査し処理する場合の概要を示すフローチャートである。

【図8】映画等の放送内容を検査し処理する場合の概要を示すフローチャートである。

【図9】ユーザー端末側の処理概要を示すフローチャートである。

【図10】ユーザーの意思によって本情報保証サービスのセット、リセットが自由にできる状態を示す説明図である。

【図11】情報安全化装置をインターネット接続事業者に適用した場合の説明図である。

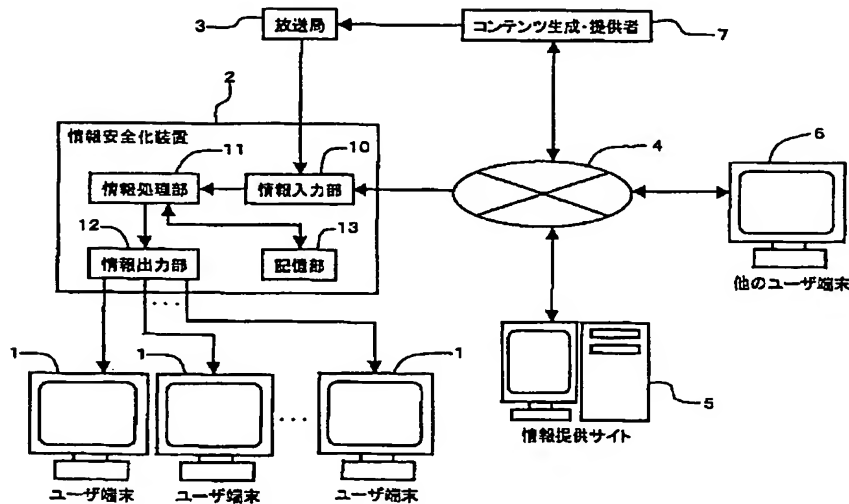
*20

*【図12】コンテンツ生成方法の概略を示す流れ図である。

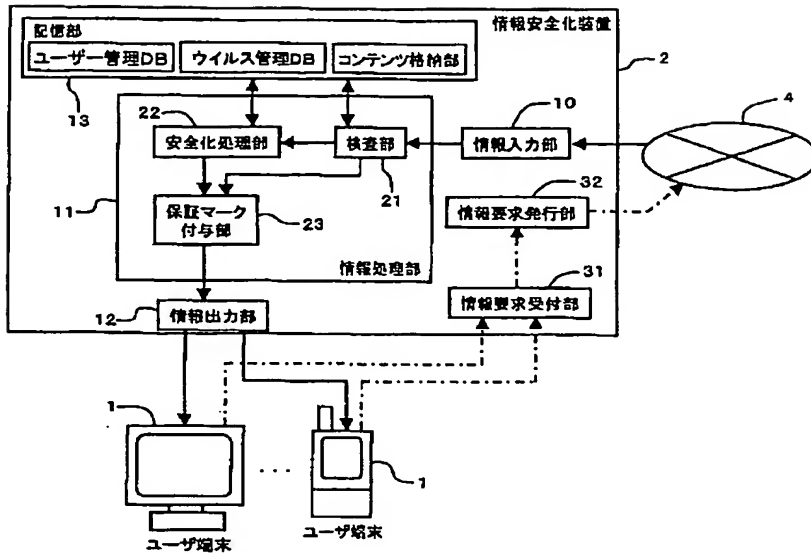
【符号の説明】

- 1 ユーザー端末
- 2 情報安全化装置
- 3 放送局
- 4 通信ネットワーク
- 5 情報提供サイト
- 6 他のユーザー端末
- 7 コンテンツ生成・提供者の装置
- 10 情報入力部
- 11 情報処理部
- 12 情報出力部
- 13 記憶部
- 21 検査部
- 22 安全化処理部
- 23 保証マーク付与部
- 31 情報要求受付部
- 32 情報要求発行部

【図1】

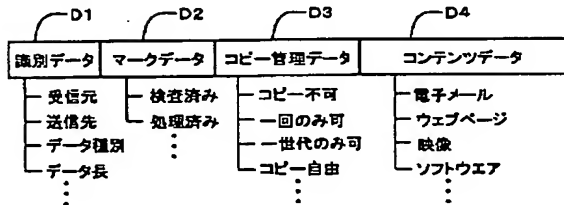


(図2)

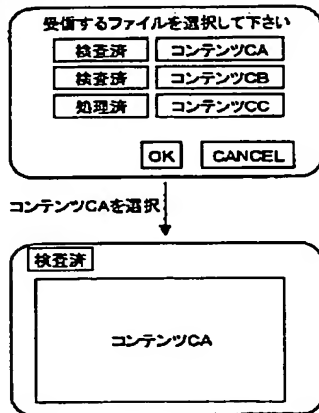


(図3)

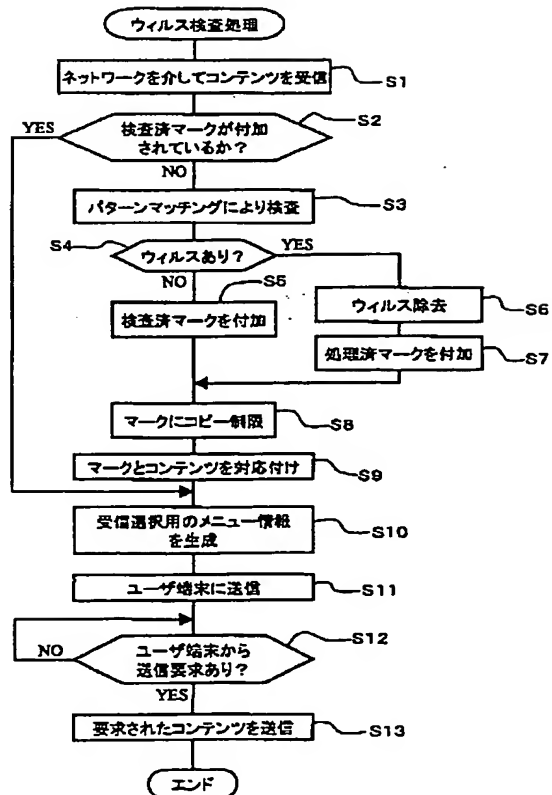
(a)データ構造



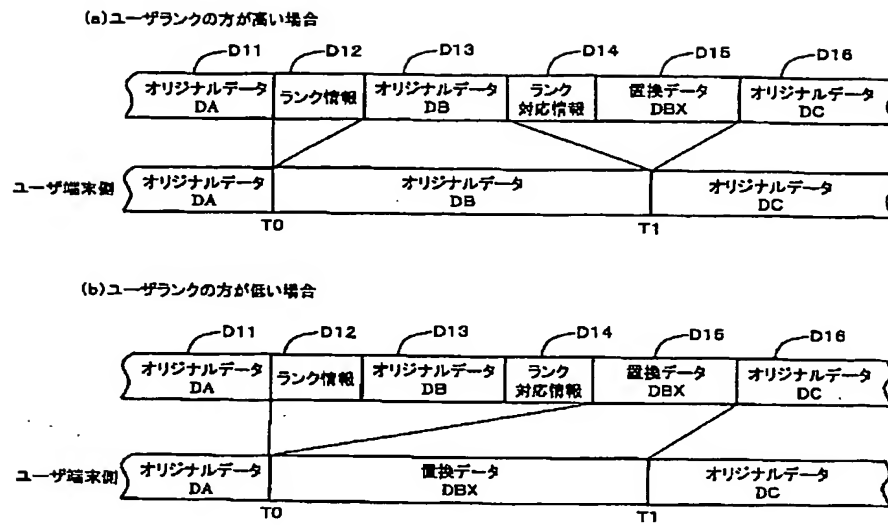
(b)ユーザー端末での表示方法



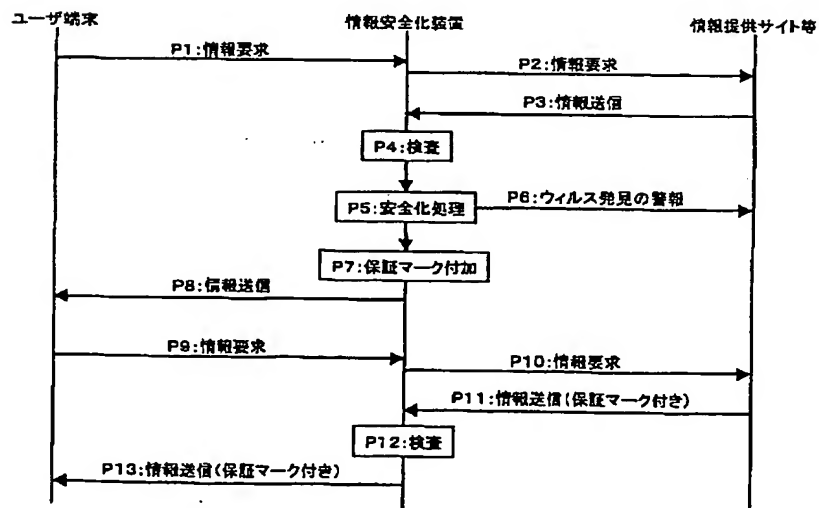
(図7)



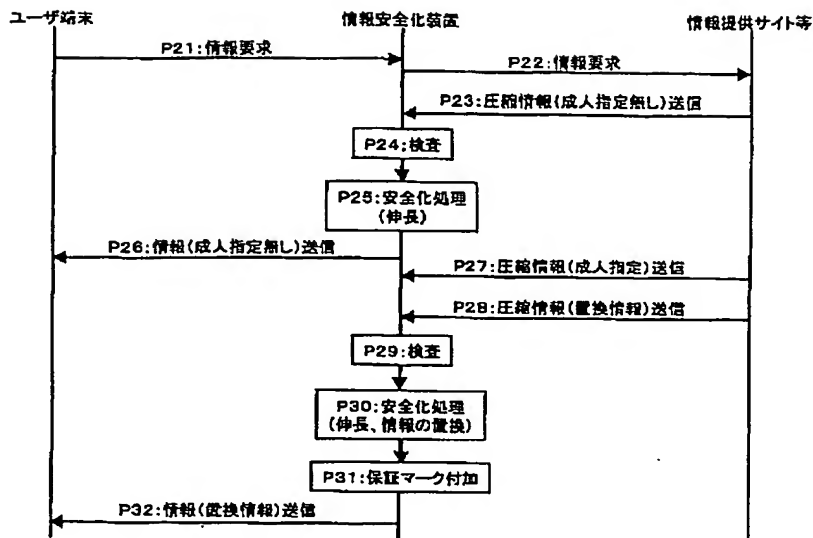
【図4】



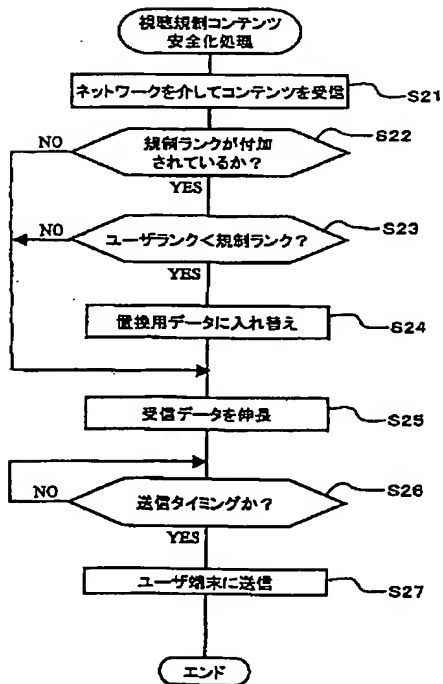
【図5】



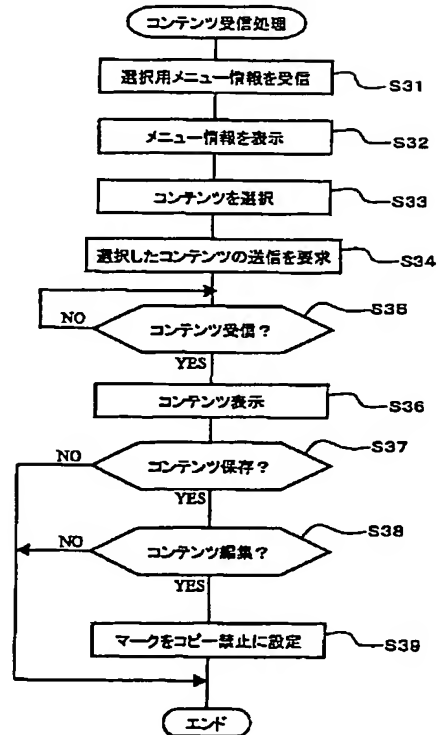
【図6】



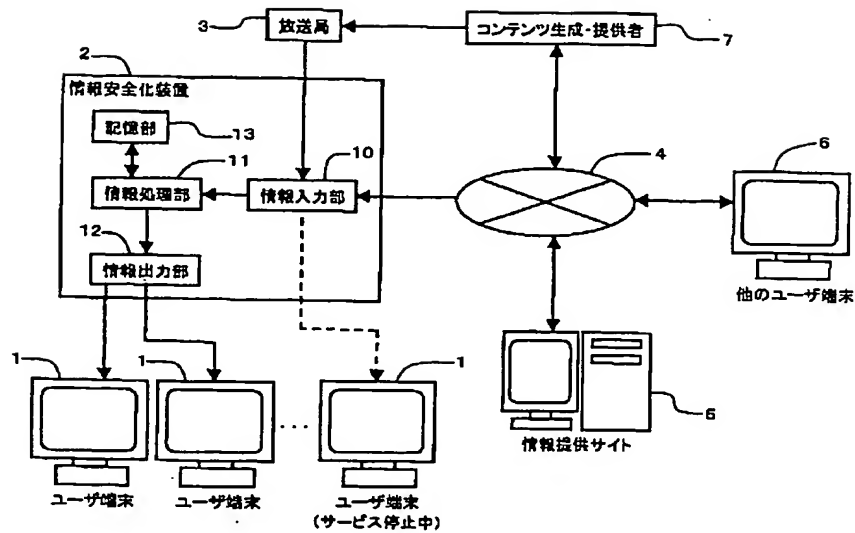
【図8】



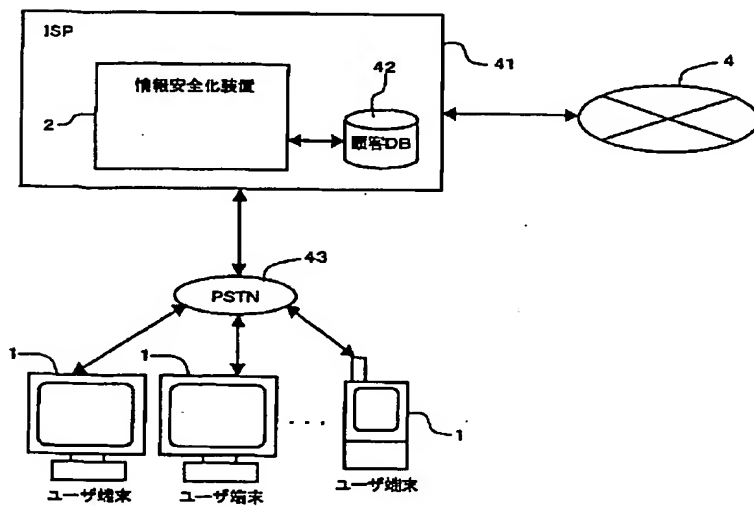
【図9】



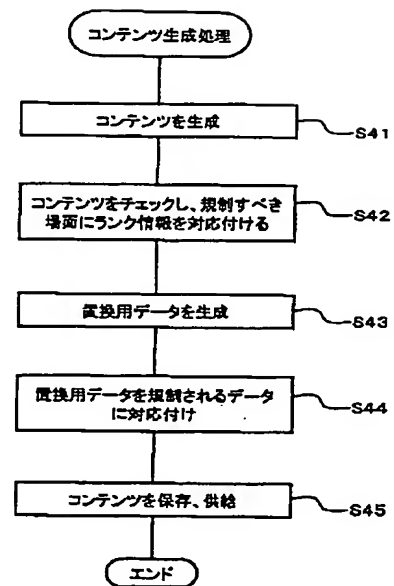
【図10】



【図11】



【図12】



This Page is inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☒ BLACK BORDERS
- ☒ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☒ FADED TEXT OR DRAWING
- ☒ BLURED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLORED OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REPERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.

**As rescanning documents *will not* correct images
problems checked, please do not report the
problems to the IFW Image Problem Mailbox**